REMARKS

This amendment responds to the Office Action dated October 3, 2005 and the interview conducted on December 8, 2005. The examiner has previously provisionally withdrew certain claims (48-62, 78-89 and 153-160) from consideration because no generic claim was allowed. As stated later, applicant respectfully requests that the examiner find that the presently amended independent claims (63, 90, 224) are patentable and reinstate claims 48-62, 78-89 and 153-160 provided applicant amends those claims in accordance with claim 63 herein.

At the interview, the examiner indicated that proposed claim 63 was patentable and distinct over the cited references but also indicated that an additional search was necessary. This amendment conforms to the interview.

In this amendment, responsive to the final Office Action dated October 3, 2005, applicant has combined independent claim 63 with the "multi-level security" portions of claim 68, which claim was argued as being patentable in the previously filed amendment. Independent claims 90 and 224 have been amended in the same manner.

In summary, Kirshenbaum '298, Lamm '907 and/or Fahlman '080 do not show, teach or suggest multiple extractions of security sensitive words related to each of a plurality of security levels, separate storage of those security sensitive words in different secured locations for each security level, storage of remainder or non-secured data in a different computer (not with the extract stores), the requirement that the user input a password ("security clearance") for each security level in order to (i) obtain access to the secured words at that security level and (ii) permit full or partial reconstruction of extracted data and

remainder data "after presentment of respective ones of said plurality of predetermined security clearances." Claim 63.

The advantages of the multiple security level - multiple dispersal and storage claim are:

- distributed, secure storage of multiple levels of secure data

- less risk of loss of secure data by attacks (intrusions) due to the dispersed storage of data

- system provides more physical barriers to electronic intrusions into storage sites

- avoids single point of machine-security clearance failure (possible with prior art systems)

- enhances the greater sharing of data by granular separation and dispersed storage of data at multiple levels of security

Kirshenbaum '298 does not show separate storage of secured data, separate and apart from unsecured data. Both secured and non-secured data is stored in a single database 14. Col. 3, lines 40-44; col. 5, lines 7-10 ("The data set is stored in a database ... the document comprises secure portion and non-secure portions"); col. 5, lines 36-37 ("to retrieve those secure and non-secure portions of the document and to send the retrieved portions of the document to the output device.").

Kirshenbaum '298 does not have "storing ... said remainder [non-secret] data in said remainder store." Claim 63. Kirshenbaum '298 teaches away from this claimed aspect of the invention.

Kirshenbaum '298 does not show extraction of multiple levels of secured data from a document. At best, Kirshenbaum '298 discloses scanning and identification of identifying codes but the identifier codes are not secured data. "In a particular embodiments, the processor is configured to identify a security clearance level of a user and then to enable the user to print portions of a document at any security level below the user's level." Col. 5, line 54. "The identifier codes printed on non-secure portions of a

document are machine readable ... and are provided to a processor by extracting the identifier codes from the machine readable format with a scanning machine." Col. 5, line 64 - Col. 6, line 1.

The present invention requires multiple security levels, each having a sub-set of security sensitive words, extraction and storage of multiple security levels, a plurality of predetermined security clearances, a particular security clearance needed to access "respective ones of said extract stores" which extract stores are active "for respective ones of said plurality of security levels." Claim 63.

In the present invention, different security clearances must be input for access to each extract store (each security level storage facility) in order to obtain the data and permit full or partial reconstruction "after presentment of respective ones of said plurality predetermined security clearances." Therefore, the present invention requires multiple extraction, each extraction for each security level, separate storage thereof, storage of the remainder or non-secured data ("storing ... said remainder data in said remainder store"), "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and, permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment of respective ones of said plurality of predetermined security clearances." Claim 63.

Fahlman '080 does not show, teach or suggest a remainder store for non-secured data, multiple security levels, multiple extraction of security data, storage of multiple levels, presentment of different security codes at each security level. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

In Fig. 1, step 111 of Fahlman "automatically" merges sensitive information into non-sensitive information. In FIG. 2, step 217, the Fahlman system again "automatically" merges secured data with un-

secured data. Fahlman discusses merging secured data with unsecured data at col. 2, line 22, col. 2, line 34, and col. 2, line 49, and col. 2, line 54 and col. 2, line 40. Fahlman '080 discloses identifying security information and extracting that information and replacing it with place holders. Col. 2, line 37 and col. 3, line 47. "The sanitized message is then transmitted with a low level of security." Col. 3, line 54. The sensitive information is stripped from the original message and stored in a separate location or together with the sanitized message. Col. 3, line 64. A map showing the location of the security information is also stored with the secured information. Col. 3, line 63. "Then, in step 111, the sensitive terms received from the second path are merged with the sanitized message to create a final confidential message." Col. 4, line 1. The examiner should note that Fahlman does not discuss reconstruction or merger in the presence of any type of security clearance. In contrast, the present invention requires multiple security clearances, each unique to a security level. Fahlman also discusses: "Then, in step 217, the sensitive terms are automatically merged back into the serviced message to create a final message." Col. 5, line 27. No discussion of multi-level security clearance is noted. The same is true regarding merger of security information and non-secured information at col. 6, line 62.

Fahlman does not seem to store remainder or non-secure data in a separate remainder store location apart from secure data. Fahlman (1) identifies secret words, (2) replaces the words with placeholders, then (3) transmits the "sanitized message." Fig. 1, step 107, Fig. 2, step 209, col 2, line 19, col. 2, line 34, col. 2, line 49, col. 3, line 54 (transmission - no storage of non-secure data), col. 4, line 64 (transmission - no separate storage). Fahlman does discuss storing the sanitized message, that is, the non-secure data and the placeholders, but not separate storage of the remainder data. Col. 3, line 63, col. 4,

line 47, col. 5, line 1. In the present invention, remainder, non-secret data is stored separately from secret data. See claim 63, "storing" step. Fahlman teaches away from this aspect of the present invention.

Fahlman does not discuss multiple security levels nor multiple storage sites at each security level. Since multiple security levels are not addressed in Fahlman, multiple security clearance codes to obtain "access" to the secured data levels is not discussed. Since Fahlman does not use any type of password or security clearance procedures, there is no "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and, permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment of respective ones of said plurality of predetermined security clearances." Claim 63.

There is no motivation nor suggestion to combine Kirshenbaum's presentment of a security code with Fahlman's single level extraction and storage of secret data. There is no suggestion nor motivation to use security codes "to obtain access" to multiple extract stores, nor reconstruct "full or partial" data in the presence of such security codes.

Lamm '907 stores and has multiple copies of all secret-secured data about the consumer in three (3) different computers, to wit, consumer computer 12 (see legends FIG. 2, consumer computer 20, col. 5, line 48), billing - processor computer 26 (see col. 13, line 5) and enrollment server 21 (see col. 9, line 42). The three computers in Lamm '907 provide an integrated bill payment system which cannot be deconstructed into operable components. In contrast, the present invention extracts secured data, for multiple security levels, and then stores "said extracted data in extract stores corresponding to a respective

security level and said remainder data in said remainder store." Lamm's process of storing secret data in three computers is completely different than the claimed system of storing secret data in multiple, "extract stores for respective ones of said plurality of security levels."

Because Lamm '907 stores secret and non-secret data in multiple locations, Lamm teaches away from the basic concept of the entire invention, that is, secure, dispersed, distributed storage of data, which can only be "reconstructed" under several password controls.

First, Lamm '907 does not have a single remainder store for non-secure data. Lamm does not have separate storage of secret data, separate and apart from non-secret data.

In Lamm '907, the non-secret or non-sensitive data is transmitted via Internet 28 and is merged with secret data by all three computers completely independent of each other, operationally or otherwise. In other words, a 1st user on consumer computer 12 can reconstruct the data with secret and non-secret data without a security code (col. 12, line 10), [1] completely separate and apart from 2nd user on billing-processor computer 26 (col. 9, line 62). [2] The claimed invention uses multiple secret-extract stores which store different data. To reconstruct a singular document, 1st and 2nd users must access the same extract store at the same security level.

---

[1] "This information from the secured billing information database 38 can appear on the reconstructed bill 154 even though it was not sent with the non-sensitive billing information to the consumer's computer 12, because it is stored locally on the consumer's computer 12. An encryption program 36 may be used on the consumer's computer 12 if data sent from the processing computer system 20 is encrypted." Col. 12, lines 36-43 (emphasis added).

[2] "As noted earlier, an authentication identifier, such as an EPO-mail address supplemented by a password [sent by the consumer], is set up to allow the processor or billing party to receive payment instructions from a consumer without the transfer of secured billing information." (col. 9, line 62)

In Lamm '907, there is no "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores" because the secret data is stored locally at all locations. Lamm does not require nor need to present a security code prior "to obtain[ing] access to ... said extract stores." (claim 63). Since the secret data in Lamm is on all three computers, there is no need to present a security code clearance, nor is there a need to present multiple "security clearances to obtain access to respective ones of said extract stores." Claim 63. Lamm does not reconstruct data "only in the presence of said predetermined security clearance after presentment" because each computer locally stores secret data and non-secret data thereon.

The prime purpose of Lamm '907 is as follows: "A primary consequence of this distinction is that billing messages 18 are prepared and sent by the processor server computer system 26 to the electronic post office 16 with redacted content only. Similarly, payment instruction messages 19 are prepared by consumer computer 12 and sent to the electronic post office 16 with redacted content only." Col. 6, lines 25-32. Lamm is not concerned with (a) extraction, (b) secure storage of extracted data at multiple levels, (b) presentment of multiple security codes for each level, (d) full or partial reconstruction "only in the presence of said predetermined security clearance after presentment". Claim 63. Lamm does not require a high level of security because the security objective of Lamm '907 is limited to protection of the sensitive information while the information travels the internet or phone wires. Lamm does not consider the storage at the three computers unsafe because it does not even require a password to access that secret information.

A combination of Kirshenbaum '298, Lamm '907 and/or Fahlman '080 would result in a three headed monster with no discernable utility. No reference specifically discusses separate storage of non-

secret, remainder data, apart from secret data. No reference shows, discusses or suggests multiple security levels and multiple stores for each level of security. Lamm stores secret data and non-secret data locally on many computers. Kirshenbaum stores all data, secret and non-secret, in one location. Fahlman extracts only a single level of data and stores it separately from the non-secure data (which is transmitted, not stored "in a remainder store" as per the claimed invention) but never discusses password control to access either type of data. It is respectfully submitted that it is improper to select disparate parts from each of these complicated systems and "cobble together" the claimed invention. There is no suggestion nor motivation to do so absent the disclosure of the present invention.

Each of the references, Kirshenbaum '298, Lamm '907 and/or Fahlman '080, describe complete systems and there is no reason to add to or substitute portions of one disclosure with another. For example, there is no reason to combine Lamm's bill paying system with Kirshenbaum's singular document storage and reproduction system and/or Fahlman's secret transmission system.

With respect to Schneier's book (Applied Cryptography), Schneier does not show, teach or suggest multi-level extract stores nor "presenting a predetermined security clearance to obtain access to said extract store; and, permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof." Schneier discusses encryption and key destruction.

Kluttz '161 does not show, teach or suggest multi-level extract stores nor presenting a predetermined security clearance to obtain access to the extract store and permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof as required by the present invention. Kluttz '161 shows utilizing

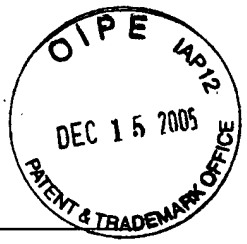
multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

Contrary to the examiner's understanding of Kluttz '161, the disclosure does not show "different levels of security for subsets of information," Office Action dated Oct. 3, 2005, p. 6. It discloses "dividing the document into at least a first portion having a first security level and a second portion having a second security level" and then encrypting these two levels differently. There is no different storage of different secure information with different password keys for each level, AND separate storage of remainder, non-secure data as per claim 63.

U.S. Patent No. 5,036,315 to Gurley does not cure the defects identified above with respect to Lamm '907 and the differences with respect to the present invention. Gurley does not show, teach or suggest (a) filtering data; (b) utilizing an extract store and a remainder store; (c) presenting a predetermined security clearance to obtain access to said extract store; and (d) permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof. Gurley '315 discusses a video display control which accepts and processes two (2) video signals, one displayed in a defined window of the second video display.

Applicant respectfully requests that the examiner approve the patentability of claims 63-77; 90-101 and 224-234. Applicant respectfully requests that the examiner permit applicant to amend the other independent claims in elected invention Group II, that is, independent claims 48, 78 and 53, to conform

to claim 63 (relative to multi-level security systems) since most of these claims 48, 78 and 153 (and dependent claims) become generic and patentable upon allowance of claim 63.



Respectfully submitted,

By _____

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Fort Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on December 13, 2005.

_____

Robert C. Kain, Jr.
Reg. No. 30,648

\\Tiger\data share\RCK\CLIENTS\Redlich\Patents\6851-02-amdt-121205.wpd